We Claim:

1. A system for access control comprising:

a database, said database including, a user interface having means to generate key codes and add user codes whereby issuing a security code with user defined parameters,

a control device having;

independent and isolated operation from said database, the control device further including,

an input device for entering security codes,

a multitude of key codes stored in memory equivalent to key codes generated by said database and,

a controller with programming having means to compare key codes inputted, to key codes in memory and, when equal, interpret the user code whereby performing a required output relative to the user code parameters.

2. The system as set forth in claim 1, wherein said ~~use~~ user codes are defined by user input via a user interface.

3. The system as set forth in claim 2, wherein said user input may be selected from a group consisting of personnel identification, time based, multiple use, single use, location based, or limits set for a peripheral device.

4. The system as set forth in claim 1, wherein the database may reside on a computing device selected from a group consisting of a personal computer, a handheld computing device, or a server.

5. The system as set forth in claim 1, wherein said key codes and said ~~use~~ user codes are cryptically embedded within said security code.

6. The system as set forth in claim 1, said database further includes a software program and algorithm having means to regenerate key codes to new key codes after being issued.

7. The system as set forth in claim 1, said database further includes a software program having means to accept input of transaction specific data associated with each security code issuance.

8. The system as set forth in claim 1, wherein said input device being selected from a group consisting of a keypad, a card reader, a barcode reader, a radio frequency transmitter, an infrared transmitter or an auxiliary input device.

9. The system as set forth in claim 8, wherein said auxiliary input device being selected from a group consisting of relays, switches, sensors, potentiometers, gauges or controls.

10. The system as set forth in claim 1, the access control device further including a software program having means to archive security codes after use.

11. The system as set forth in claim 10, the software program further including an algorithm having means to regenerate key codes to new key codes equal to newly regenerated key codes in the database.

12. The system as set forth in claim 1, said access control device further including a software program having means to limit the amount of key codes in memory available for comparison to the inputted security codes from the total amount of security codes in memory.

13. The system as set forth in claim 1, the access control device further including a software program having means to recognize valid security codes inputted when said security codes are inputted in a different sequential order than issued from the database.

14. The system as set forth in claim 1, the access control device further including a software program having means to interpret the user defined parameters of the inputted ~~use~~ user code and perform a function relative to the user code parameters.

15. A method for access control comprising:

utilizing a computer program and database to obtain a unique key code, add a use code comprised of user defined parameters and provide the resulting security code to an access control user,

said access control user inputs the security code into an access control device via an input device, said access control device having key codes stored in memory equivalent to said key codes stored on the database, said access control device further including a software program having means to limit the amount of key codes in memory available for comparison to inputted security codes from the total amount of key codes in memory, said access control device compares inputted key codes to those in memory and if valid, interprets the use code portion of the security code to perform a required output.

16. The method as set forth in claim 15, wherein said user defined parameters may be selected from a group consisting of, personnel identification, start time, stop time, elapsed time, multiple use, single use, location of use, or limits set for a peripheral device.

17. The method as set forth in claim 15, the database further including a software program and algorithm with means to regenerate key codes to new key codes after being issued.

~~18. The method as set forth in claim 15, the access control device further including software program having means to limit the amount of key codes in memory available for comparison to inputted security codes from the total amount of key codes in memory.~~

~~19.~~ 18. The method as set forth in claim 15, the access control device further including a software program and algorithm having means to archive used security codes and regenerate key codes to new key codes equal to newly regenerated key codes in the database.

~~20.~~ 19. The method as set forth in claim 15, the access control device further including a software program having means to recognize valid security codes inputted when said security codes are inputted in a different sequential order than issued from the database.